IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

JAMES R. KLUMB,	)	
	)	
Plaintiff(s),	)	
	)	
v.	)	**Case No. 2:09-cv-115**
	)	***Judge William B. Mitchell Carter***
CRYSTAL GOAN,	)	
	)	
Defendant.	)	

Memorandum and Order

I. Introduction

Defendant Crystal Goan's motion for summary judgment (Doc. 39) is pending, and the Court is asked to decide whether the defendant violated the federal Wiretap Act, 18 U.S.C. § 25110 *et seq.*, and the Tennessee Wiretap Act, Tenn Code. Ann. § 39-13-601 *et seq.,* when she placed spyware on two computers used by her husband, the defendant, to intercept his incoming and outgoing e-mail and to monitor his activities on the internet. The Court concludes that the keylogging function did not violate the Wiretap Act but that there is a genuine issue of material fact as to whether other functions of the spyware unlawfully "intercepted" the plaintiff's incoming and outgoing e-mail thereby violating the Wiretap Act. Further, a genuine issue of material fact also exists as to whether the plaintiff consented to the interception of his e-mail and other computer activities. Therefore, the Court will GRANT in part and DENY in part defendant's motion for summary judgment.

II. Relevant Facts

Roy Klumb and Crystal Goan used to be married. They wed on April 29, 2006. During all times relevant to this lawsuit, Roy worked at the family business, Klumb Lumber Company, Inc., which owned at least four personal computers in the office where Roy worked. Sometimes Roy let Crystal use the computers. Roy also let his two children from a previous marriage use the computers.

On June 12, 2006, Crystal installed a spyware program called eBlaster on one of the computers Roy used at work. Crystal was able to install the spyware program because Roy had given her the administrative password for the computer. Subsequently, on June 27, 2007, Crystal installed eBlaster on another computer at her husband's office using the administrative password provided by him.

Crystal asserts that she and Roy agreed to put the spyware on the first computer to track the activity of Roy's children. Roy denies this assertion. Crystal also stated in her deposition that she installed the spyware program on the second computer because she believed her husband was having an affair. (Crystal Goan dep. at 28, Doc. 43-6, Page ID # 313). While it is undisputed that Roy had given Crystal permission to use the computers at issue and gave her the administrative password for the computers, Roy denies he gave her permission to install the spyware or to access his e-mail. Roy alleges in his complaint that he first became suspicious "about Goan's installation of unauthorized Internet spyware in November 2007 when he compared hard copies of his original email communications to an email recipient to later emails to that same recipient, and discovered that the original email communications had been intercepted, tampered with, and re-sent to the original recipient by Goan." (Complaint ¶ 11, Doc.

16-1, Page ID #62). Roy eventually retained a computer forensics expert who discovered the spyware on the two computers. Roy and Crystal divorced on February 17, 2009. Roy alleges Crystal attempted to use these emails to her advantage in the divorce. *Id.* at Page ID # 63.

eBlaster is a product of SpectorSoft Corporation. (Deposition of Ronald Chesley, VP of SpectorSoft Corp. at 5, Doc. 39-4, Page ID # 185). eBlaster is a computer monitoring software installed onto a computer's operating system, such as Windows, that records the computer user's activities, aggregates that information into a report, and periodically e-mails that report to a configured e-mail address. (*Id.* at Page ID # 186-87). The eBlaster program has several features: (a) it has a keystroke recording application, *i.e.* it will record every keystroke the computer user makes on the keyboard. This features does not require internet hookup (Chesley dep. 46, Doc. 39-4, Page ID #188; Plaintiff's Response to Defendant's Statement of Material Facts, No. 12, Doc. 45, Page ID #343; William Dean dep. at 34, Doc. 39-2, Page ID # 167; Kent Copp Report, Doc. 39-6, Page ID# 196-97), (b) it can forward e-mail as soon as the computer receives it (William Dean dep. at 23, Doc. 39-2, Page ID # 162; Dean Investigative Report, Doc. 43-3, Page ID # 269), (c) it can "capture" incoming and outgoing chat messages, incoming and outgoing e-mail, and peer to peer searches, *i.e.* the downloading of applications and software, and show what websites were visited (William Dean dep. at 23-24, Doc. 39-2, Page ID # 162-63; Dean Investigative Report, Doc. 43-3, Page ID # 271), (d) it prepares a report of all activity on the computer (Chesley dep. at 46, Doc. 39-4, Page ID # 188 , Dean dep. at 23, Doc. 39-2, Page ID #162) and (e) it sends a copy of the report to an e-mail address designated by the person who installed the spyware program. This function does require connection to the internet. (Chesley dep. at 46, Doc. 39-4, Page ID # 188; Dean dep. at 23-24, 34, Doc. 39-2, Page ID # 162-63, 167;

Plaintiff's Response to Defendant's Statement of Material Facts, No. 12, Doc. 45). According to plaintiff's forensics computer expert, William Dean, who examined the two computers at issue, all these functions were enabled at the time he examined the computers and eBlaster was configured to send a report every 60 minutes to the following address: cmgoan@yahoo.com. (Dean Investigative Report, Doc. 43-3, Page ID #s 269-73, 282-84). Defendant does not dispute that this address was her email address.

Finally, the parties' experts disagree as to what point in the e-mail communication process the eBlaster program accessed, intercepted or recorded e-mail outgoing and coming into the two computers at issue. *See* David Tarnoff Report, Doc. 39-7, Page ID# 203 ("it is impossible for applications such as monitoring software to attach themselves to the hardware and capture data as it passes through the communications network.") *Cf.*, Affidavit of William E. Dean, Doc. 43-3, Page ID # 250 ("Mr. Tarnoff is not correct in stating that due to the nature of modern operating systems it is not possible for an installed application (software) to intercept communication of any form...When the eBlaster software is active, email sent or received is intercepted while in the Presentation and Application layers [of the Open Systems Interconnectivity (OSI)] and routed to a third party, in this case, Ms. Goan.") As will be seen later, the Court does not think this disagreement to be significant in this case.

III. Analysis

A. Standard of Review

Under Fed. R. Civ. P. 56, the Court will render summary judgment if there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. The burden is on the moving party to show conclusively no genuine issue of material fact exists, *Lansing Dairy, Inc. v. Espy*, 39 F.3d 1339, 1347 (6th Cir. 1994); *Kentucky Div., Horsemen's Benev. & Prot. Ass'n., Inc. v. Turfway Park Racing Assoc., Inc.*, 20 F.3d 1406, 1411 (6th Cir. 1994), and the Court must view the facts and all inferences drawn therefrom in the light most favorable to the nonmoving party. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986); *In re: Julian Co.,* 44 F.3d 426, 429 (6th Cir. 1995); *City Management Corp. v. U.S. Chemical Co., Inc.*, 43 F.3d 244, 250 (6th Cir. 1994).

Once the moving party presents evidence sufficient to support a motion under Rule 56, the nonmoving party is not entitled to a trial merely on the basis of allegations. The nonmoving party may not rest on its pleadings, but must come forward with some significant probative evidence to support its claim. *Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986); *Lansing Dairy*, 39 F.3d at 1347; *Horsemen's Benev.*, 20 F.3d at 1411; *see also Guarino v. Brookfield Tp. Trustees*, 980 F.2d 399, 404-06 (6th Cir. 1992) (holding courts do not have the responsibility to search the record *sua sponte* for genuine issues of material fact). The Court determines whether sufficient evidence has been presented to make the issue of fact a proper jury question; the Court does not weigh the evidence, judge the credibility of witnesses, or determine the truth of the matter. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249 (1986); *Schreiber v. Moe*, 596 F.3d 323, 334 (6th Cir. 2010);*60 Ivy Street Corp. v. Alexander*, 822 F.2d 1432, 1435-36 (6th Cir. 1987). If the nonmoving party fails to make a sufficient showing on an essential element of its case with respect to which it has the burden of proof, the moving party is entitled to summary judgment. *Celotex*, 477 U.S. at 323.

III. Analysis

B. Interception of Electronic Communication

Plaintiff brings his claims under the Wiretap Act, 18 U.S.C. §§ 2511(1)(a) and (c) and under 18 U.S.C. § 2520. Section 2520 creates a private right of action for damages for those persons whose wire, oral, or electronic communications have been intercepted, disclosed or intentionally used in violation of Section 2511.[1] Section 2511(1)(a) and (c) provide in relevant part:

> (1) Except as otherwise specifically provided in this chapter any person who--
>
> (a) intentionally ***intercepts***,... any wire, oral, or electronic communication [and/or];
>
> *   *   *
>
> (c) intentionally discloses, or endeavors to disclose ... to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the ***interception*** of a wire, oral, or electronic communication in violation of this subsection;
>
> *   *   *
>
> shall be punished ....

[1] 18 U.S.C. § 2520 states in relevant part: "Recovery of civil damages authorized (a) In general.–... any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate." Tenn Code. Ann. § 39-13-603 is Tennessee's counterpart to Section. 2520. It states in relevant part: "any aggrieved person whose wire, oral or electronic communication is intentionally intercepted, disclosed, or used in violation of § 39-13-601... may in a civil action recover from the person or entity that engaged in that violation...."

(Emphasis added).[2] Because the Tennessee Wiretap Act (TWA) is, in all respects relevant to this lawsuit, identical to the federal Wiretap Act and there is a dearth of Tennessee law interpreting the TWA, courts have relied upon interpretations of the federal Wiretap Act in order to interpret the TWA. *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp.2d 967, 979 (M.D. Tenn. 2008); *Hayes v. Spectorsoft Corp.*, 2009 WL 3713284 * 9 (E.D. Tenn. Nov. 3, 2009). This Court shall do the same.

It is undisputed that the type of communication at issue here is electronic communication. The Wiretap Act, 18 U.S.C. § 2510(12), defines electronic communications, with some exceptions not relevant here, as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...." Generally, e-mails in the process of being sent over the internet are electronic communications. *See e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005); *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir. 2004); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 460 (5th Cir. 1994); *Garback v. Lossing*, 2010 WL3733971 *2 (E.D. Mich. Sept. 20, 2010).

[2] Tenn Code. Ann. §§ 39-13-601(a)(1)(A) and (a)(1)(C) provide in relevant part:
a person commits an offense who:

(A) Intentionally intercepts, ... any wire, oral, or electronic communication;

* * *

(C) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection (a)....

The focus of this motion centers on the definition of "intercept" as it is used in Section 2511(1)(a) and (c). The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). As will be seen shortly, the language of this definition is considered by many jurisdictions to be incomplete. Unfortunately, there is no Sixth Circuit or Supreme Court decision to steer this Court to its conclusion. A majority of courts that have examined the definition of "intercept" as defined by the Wiretap Act have concluded that in order for electronic communications such as e-mails to be "intercepted," they must be acquired contemporaneously with transmission of the e-mails. *See Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3d Cir. 2004):

> Every circuit court to have considered the matter has held that an "intercept" under the ECPA must occur contemporaneously with transmission. *See United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir.2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir.2002); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir.1994); *see also Wesley College v. Pitts*, 974 F.Supp. 375 (D.Del.1997), *summarily aff'd*, 172 F.3d 861 (3d Cir.1998).

Id. at 113. *See also*, *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp.2d 967, 979-80 (M.D. Tenn. 2008) (acquisition of e-mail must occur while the e-mail is "in flight" in order for it to have been "intercepted" within the meaning of the Wiretap Act.) Generally, this interpretation of "intercept" means an electronic communication cannot be "intercepted" while it is in electronic storage, even temporary storage, because it is not "in flight" or acquired "contemporaneously with transmission" at that time.

The rational used by courts for this "in flight" interpretation of "intercept" is stated succinctly in *Cardinal Health*, 582 F. Supp.2d at 979-80:

> [First] there is the statutory history, which shows that Congress created the SCA [Stored Communications Act] for the express purpose of addressing "access to stored ... electronic communications and transactional records." [*Konop*, 302 F.3d] at 879 (citing S. Rep. 99-541 at 3) (emphasis added). [Second], until October 2001, the definition of "wire communication" in the FWA [Federal Wiretape Act] included information in electronic storage, such as a voicemail, but the definition of "electronic communication" in the FWA did not include information in electronic storage, indicating that something like an e-mail would not be covered by the FWA. *Id.; Fraser*, 352 F.3d at 114. Further, after 9/11, Congress amended the FWA to eliminate communications in electronic storage from the definition of "wire communication," further indicating a congressional intent that the FWA should be primarily concerned with information in active transport, not stored information. *Id.*

The factual scenarios of those cases in which other circuits have adopted this narrow, bright-line interpretation of "intercept" fit comfortably into the interpretation's limitations. *See Steve Jackson Games*, *Inc.*, 36 F.3d at 461-62 (5th Cir. 1995) (the Secret Service's unauthorized access to e-mails already posted on an electronic bulletin board did not violate the Wiretap Act); *Konop*, 302 F.3d at 878 (defendant's unauthorized access to a restricted website did not violate the Wiretap Act); *Steiger*, 318 F.3d at 1050-51 (hacker who used a Trojan Horse virus to access photographs stored in another person's computer did not violate the Wiretap Act); *Fraser*, 352 F.3d at 113-14 (insurance company which searched server and accessed old copies of an independent agent's e-mails did not violate the Wiretap Act); *Cardinal Health*, 582 F. Supp.2d at 980-81 (defendant's use of wrongfully obtained password to access competitor's e-mail account to view e-mails already posted in competitor's mail-box but not yet read did not violate Wiretap Act).

However, since those cases were decided, the Seventh Circuit has examined the application of the Wiretap Act to e-mails and concluded the previous decisions' interpretations of the Wiretap Act are too narrow because they fail to properly consider the realities of how e-mail is actually transmitted over the internet and Congress' intent in prohibiting interception of such transmissions. In *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010), the defendant, Szymuszkiewicz, was concerned he was going to be fired, so he accessed his supervisor's workplace computer when she was away from her desk and entered a "rule" onto her e-mail client, Microsoft Outlook, to automatically forward all his supervisor's incoming e-mails to him. All the supervisor's incoming e-mails went first to their employer's server in a different city. Then, at some point, either at the server level or at his supervisor's computer, a copy of the incoming e-mail was automatically made and sent to Szymuszkiewicz's e-mail address. The Seventh Circuit concluded that, for purposes of the Wiretap Act, it did not matter whether the copy sent to Szymuszkiewicz was made by the server or by the supervisor's own computer– both constituted a violation of the Wiretap Act. "To see why," stated the Szymuszkiewicz Court, "we need to take a brief foray into the world of packet switching, the method by which nearly all electronic communications between computers are now sent:"

> When the Wiretap Act was enacted in 1968, the normal communications pathway was circuit switching: the telephone company's machinery (initially switchboards, then mechanical solenoids, and finally computers) would establish a single electronic pathway, or circuit, between one telephone and another. Computers can communicate over dedicated circuits, but usually they break each message into packets, which can be routed over a network without the need to dedicate a whole circuit to a single message.
>
> Each packet contains some of the message's content, plus information about the packet's destination. Each packet travels independently, moving from router to router within a network to find a path toward the ultimate destination. .... The routers, and the computers on both ends, arrange the packets (and their address information), and resend as necessary, so that at least one copy of each of the message's many packets reaches its goal. ... Every packet may go by a different route. Only at the end are the pieces put back together and an intelligible communication formed. The path of any particular packet, and the order in which it arrives at the end, is irrelevant to the success of the communication. Computers

> use a recipe known as a protocol that enables them to agree on how packets are formatted and reassembled.

Szymuszkiewicz, 622 F.3d at 704. In eschewing Szymuszkiewicz's argument that there could be no wiretapping because the incoming e-mail messages were not intercepted before they reached the supervisor's computer, the Seventh Circuit stated,

> Szymuszkiewicz's understanding of "interception" as "catching a thing in flight" is sensible enough for football, but for email there is no single "thing" that flies straight from sender to recipient. When sender and recipient are connected by a single circuit, and the spy puts a "tap" in between, the football analogy makes some sense (though the tap does not prevent the recipient from getting the message; the spy gets a copy, just as Szymuszkiewicz did). *For email, however, there are no dedicated circuits. There are only packets, segments of a message that take different routes at different times.*

(Emphasis added). The Court noted that had the supervisor and Szymuszkiewicz been sitting at their computers at the same time, "they would have received each message with no more than a blink of an eye between. That's contemporaneous by any standard," and that even if the supervisor's computer was doing the copying and forwarding, "it was effectively acting as just another router, sending packets along to their destination." *Id.* at 706. The *Szymuszkiewicz* court concluded, "the Wiretap Act applies to messages that reside briefly in the memory of packet-switch routers...." *Id.(citing United States v. Councilman,* 418 F.3d 67 (1st Cir.2005) (en banc)("We conclude that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications.")) Thus, the *Szymuszkiewicz* court concluded Szymuszkiewicz had been properly convicted of wiretapping.

The District Court in *Potter v. Halicek,* 2007 WL 539534 *2 (S.D. Ohio Feb. 14, 2007) took an even more expansive approach to the Wiretap Act. In *Potter*, the defendant installed spyware on the plaintiff's computer which logged all her keystrokes and took a screen shot of all incoming e-mail after it reached her computer. The key logging function records entirely internal transmissions from the keyboard to the computer's CPU. Nevertheless, focusing on theWiretap Act's requirement that the electronic communications must affect interstate commerce, the court found that logging key strokes which are used to send a message off into interstate commerce and that making screen shots of the incoming e-mail which has traveled over the internet constitute a violation of the Wiretap Act. *Id.* at 8. *Potter* is the only case the Court could find which suggests that use of key logging spyware may violate the Wiretap Act, and the undersigned declines to adopt so broad an interpretation of the Wiretap Act.

Instead the Court adopts the router switching analysis relied upon in *Szymuszkiewicz*. Programming a computer, either through the use of spyware or legitimate means, to automatically forward an e-mail upon receipt by one e-mail account to another e-mail account requires that the e-mail be transmitted twice over the internet. First, the sender transmits the e-mail, in packets, to the intended recipient through the internet. At the intended recipient's computer, the e-mail is automatically copied and launched again into the internet, in packets, to be transmitted to the third party's e-mail account. That the e-mail may have rested momentarily in the intended recipient's account before being transmitted back though the internet to the third party is of no consequence. That the recipient and the third-party might access their respective e-mail accounts on the same computer is immaterial. The e-mail has still been captured and re-routed within a "blink of an eye" through the internet to someone who was not authorized to have it. That is contemporaneous enough.

The Court now turns to the case at hand. The defendant seeks to turn the Court's attention to the keylogging function of the eBlaster program. The keylogging function records all keys typed on the keyboard. It does not use the transmission of any form of electronic communication over the internet to make such records; therefore, it cannot, as a matter of law, violate the Wiretap Act. Thus summary judgment as to the key logging function will be granted.

On the other hand, this case is similar to *Szymuszkiewicz* in that plaintiff has presented evidence in this case that eBlaster directed that all incoming e-mails to plaintiff's account automatically be copied and forwarded to the defendant. Defendant argues this case is significantly different from *Szymuszkiewicz* because Szymuszkiewicz used "an intermediate device, his boss's computer, to re-route the data." (Defendant's Reply brief at 2, Doc. 48, Page ID # 357). As previously discussed, the Court finds this fact insignificant. Forwarding plaintiff's e-mail to defendant's e-mail account requires the e-mails to be transmitted from the plaintiff's e-mail account in packets through the internet before coming back to rest in the defendant's e-mail account. The point is that plaintiff's e-mails were automatically routed by an electronic device (the Klumb Lumber computers) through the internet to the defendant's e-mail account.

As to outgoing e-mail and screen shots of e-mail, the defendant has not presented a clear picture to the undersigned as to how the defendant accessed them. Without clearly understanding how the outgoing e-mails and the screen shots were captured and presented to the defendant, the Court declines to grant summary judgment as to this issue.

C. Consent

Section 2511(c) of the Wiretap Act provides, "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."[3] It is undisputed that plaintiff gave the defendant his administrative password for the two computers at issue which permitted the defendant to install software on the computer. Had the plaintiff only given the defendant a user password, she could have used the computer but not installed software.

Defendant argues that when plaintiff gave her the administrative passwords for the two computers at issue, in effect, plaintiff was consenting to her installing any program she wanted to on the computers including the spyware to intercept his e-mail. Defendant has cited no authority for that position, and the Court did not find a single case holding that revealing an administrative password was the equivalent, as a matter of law, of permitting the installation of spyware. The plaintiff strenuously denies that he agreed that his e-mail and all activities on the computers could be monitored. There is a genuine issue of material fact as to whether the plaintiff consented to the interception of his e-mail and other electronic communications.

[3] The counterpart under the Tennessee Wiretap Act is Tenn Code. Ann. § 39-13-601(b)(5) which provides in relevant part:

> It is lawful under §§ 39-13-601 ... for a person not acting under color of law to intercept a wire, oral, or electronic communication, where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception ....

IV. Conclusion

In summation, the Court concludes (1) summary judgment is GRANTED to the extent plaintiff is alleging a violation of the Wiretap Act based on the use of the key logging function on eBlaster, and (2) summary judgment is DENIED to the extent the plaintiff is alleging a violation of the Wiretap Act for forwarding plaintiff's e-mail to defendant's e-mail address and for the screen capture function of the eBlaster program.

SO ORDERED.

s/William B. Mitchell Carter
UNITED STATES MAGISTRATE JUDGE